GEMEENTE Nunspeet

GEMEENTEBLAD

Officiële uitgave van de gemeente Nunspeet

Nr. 563678

28 december 2023

Privacybeleidskader Gemeente Nunspeet 2023-2024

1. Inleiding

Vanaf 25 mei 2018 geldt de Algemene Verordening Gegevensbescherming (AVG). De gemeente Nunspeet heeft in haar privacybeleidskader vastgelegd hoe het omgaat met de bescherming van persoonsgegevens.

De verwerking van persoonsgegevens door buitengewoon opsporingsambtenaren (boa's) valt niet alleen onder de AVG maar ook onder de Wet politiegegevens (Wpg). Daarnaast is een aantal andere regelingen van toepassing op de verwerking van politiegegevens. Zoals het Besluit politiegegevens (Bpg), het Besluit politiegegevens buitengewoon opsporingsambtenaren en de Regeling periodieke audit politiegegevens.

De AVG en de Wpg sluiten elkaar wederzijds uit. Op een aantal onderdelen is zeker ook sprake van overlap. Andere verplichtingen zijn vergelijkbaar maar kennen verschillen in de concrete uitwerking, zoals de verplichting voor de verwerkingsverantwoordelijke om passende technische en organisatorische maatregelen te treffen ter bescherming en beveiliging van de gegevens. In het kader van de Wpg is bijvoorbeeld ook eens per 4 jaar een externe audit verplicht en moeten elk jaar interne audits worden gehouden.

Het huidige privacybeleid van Nunspeet gaat alleen uit van de AVG. Het is daarom wenselijk er de verplichtingen uit de Wpg aan toe te voegen.

2. De boa's bij Nunspeet

Gemeente Nunspeet verwerkt politiegegevens onder de Wpg. De boa’s in dienst van gemeente Nunspeet voeren taken uit, die vallen onder de Wpg, voor de domeinen 1, Openbare Ruimte, 2, Milieu, Welzijn en Infrastructuur en 5 Werk, Inkomen en Zorg (Sociale recherche). De boa’s domeinen 1 en 2 verwerken de politiegegevens in de daarvoor aangeschafte applicatie BRS. Dit betreffen verwerkingen die voortvloeien uit hun taken zoals: het staande houden, het opmaken van een proces verbaal of aanhouding en verhoor. De boa’s van de Sociale recherche verwerken de politiegegevens in Word en Djuma (afgeschermde versie) en voeren de volgende taak daar in uit: strafrechtelijke handhaving van sociale zekerheidsfraude.

3. Doelstellingen van het privacybeleid

Het privacybeleidskader van Nunspeet beschrijft hoe we verantwoordelijk en binnen wettelijke kaders met persoonsgegevens omgaan. Voor de reikwijdte van dit addendum bestaat het wettelijk kader voor bescherming van persoonsgegevens uit de Wpg en de daar op gebaseerde regelingen. De gemeente Nunspeet wil met dit addendum op het privacybeleidskader onder andere bereiken dat de boa's:

- Zich ten volle bewust zijn van de noodzaak om zorgvuldig en op rechtmatige wijze om te gaan met politiegegevens;
- De rechten van betrokkenen respecteren en werken volgens de vastgestelde procedures;
- Het vertrouwen van betrokkenen in de overheid niet beschamen.
- Gedrag vertonen dat past bij goed werknemerschap.
- De kans op financiële en imagoschade minimaliseren.

4. Wpg kader

Het normenkader van de Wpg is grotendeels gelijkluidend aan dat van de AVG. Op hoofdlijnen geldt aanvullend nog het volgende:

- De boa's van de gemeente Nunspeet kunnen naast hun opsporingstaken ook bestuursrechtelijke toezichts- en handhavingstaken hebben. Zij krijgen dan bij het verwerken van persoonsgegevens zowel met de AVG te maken als met de Wpg;
- In de verwerking van gegevens moet duidelijk zijn welke gegevens er worden verwerkt onder de AVG en welke onder de Wpg. De Wpg stelt andere eisen aan de verwerking van persoonsgegevens dan de AVG. Zo geldt onder andere de plicht tot delen met ieder andere opsporingsambtenaar die deze gegevens nodig heeft voor zijn werk.

De Wpg kent een aantal verplichtingen, die veelal geborgd binnen onze applicaties:

- Er moet een scheiding worden aangebracht tussen gegevens die op feiten zijn gebaseerd en gegevens die op een persoonlijk oordeel zijn gebaseerd;

- Er moet onderscheid worden gemaakt tussen betrokkenen, zoals verdachten, slachtoffers, derden en veroordeelden;
- Documentatie is vereist van de doelen van onderzoeken, verstrekking of doorgifte, afwijzing van verzoeken om inzage, inbreuk op de beveiliging, doorgifte buiten de EU met datum en tijd, ontvanger, redenen en doorgegeven gegevens en melding van gemeenschappelijke verwerkingen aan de Autoriteit Persoonsgegevens (AP).
- Er vindt logging plaats in geautomatiseerde systemen van de invoer van gegevens in systemen en op termijn ook van het verzamelen, wijzigen, raadplegen, verstrekken (o.a. in de vorm van doorgifte), combineren of vernietigen van politiegegevens.
- Er worden specifieke eisen gesteld aan de informatiebeveiliging op basis van het Bpg.

Er geldt met ingang van 2021 een verplichting tot het uitvoeren van een externe privacy audits. De rapportage die hieruit voortvloeit moet worden verstrekt aan de AP. Als er tekortkomingen zijn geconstateerd moet 3 maanden na het uitvoeren van de audit een verbeterrapport worden opgesteld, waarop binnen een jaar een her controle plaatsvindt. De hercontrole geldt alleen voor die onderdelen van de wet waar de tekortkomingen geconstateerd worden. De resultaten van de hercontrole worden vastgelegd in een rapportage en eveneens verstrekt aan de AP, uiterlijk 1 jaar na het uitvoeren van de externe audit.

5. Register van verwerkingen

Net als de AVG verplicht de Wpg tot het bijhouden van een register van verwerkingen. Wel zijn er enkele verschillen die hierna met een (*) zijn aangeduid. Het register van verwerkingen in het kader van de Wpg moet het volgende bevatten:

- De naam en de contactgegevens van de verwerkingsverantwoordelijke, de gezamenlijk verwerkingsverantwoordelijken en de functionaris voor gegevensbescherming;
- De doelen van de verwerking;
- De categorieën van ontvangers aan wie politiegegevens zijn of zullen worden verstrekt, met inbegrip van ontvangers in derde landen of internationale organisaties;
- Een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- In voorkomend geval: het gebruik van profilering. (*)
- In voorkomend geval: de categorieën van doorgiften van politiegegevens aan een derde land of een internationale organisatie.
- Een aanwijzing van de rechtsgrondslag van de verwerking, met inbegrip van doorgiften, waarvoor de politiegegevens bedoeld zijn. (*)
- Zo mogelijk: de beoogde termijnen waarbinnen de verschillende categorieën van gegevens worden verwijderd of vernietigd.
- Zo mogelijk: een algemene beschrijving van de technische en organisatorische maatregelen ter beveiliging.
- De toekenning van de autorisaties. (*)

6. Informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid is vastgelegd in een richtinggevend en kader stellend beleidsdocument, welke eens per 4 jaar wordt vastgesteld door het college. De gemeente Nunspeet vult het aan met beleid voor informatiebeveiliging op tactisch en operationeel niveau met specifieke (beleids-) documenten.

Het informatiebeveiligingsbeleid geldt voor alle activiteiten van de gemeente. Ook voor de activiteiten die vallen onder de Wpg, geldt dat passende technische en organisatorische maatregelen moeten zijn genomen en geïmplementeerd, op basis van een risicoanalyse waaruit het risiconiveau blijkt met betrekking tot ongeoorloofde of onrechtmatige verwerking en tegen opzettelijk verlies, vernietiging of beschadiging. Deze maatregelen moeten bovendien periodiek worden geëvalueerd en zo nodig geactualiseerd.

7. FG en bevoegd functionaris

<u>De Functionaris Gegevensbescherming (FG)</u>

Net als in de AVG verplicht artikel 36 van de Wpg tot het aanstellen van de FG. Het is mogelijk dat meerdere organisaties samen één FG aanwijzen. De FG wordt door de verwerkingsverantwoordelijke tijdig en naar behoren betrokken bij alle aangelegenheden die verband houden met de bescherming van politiegegevens. De FG stelt jaarlijks een verslag op van zijn bevindingen en stelt het ter beschikking aan de verwerkingsverantwoordelijke.

<u>De bevoegd functionaris</u>

De bevoegd functionaris kan worden geworven uit de poule van functionarissen die het Samenwerkingsverband van gebruikersorganisaties (SupBRS) heeft opgeleid en die binnen de applicatie beschikbaar zijn gemaakt. De bevoegd functionaris is de ‘hoeder’ van de gegevens die onder artikel 9 Wpg

worden verwerkt. Deze functionaris is beschreven in artikel 2:10, eerste lid, van het Besluit politiegegevens (Bpg). Het moet een persoon zijn met voldoende kennis en vaardigheden over dit type gegevens. Deze functionaris beslist bijvoorbeeld wie er toegang mag hebben tot deze gegevens en of ze verstrekt kunnen worden aan een samenwerkingspartner. Iedere artikel 9-verwerking dient een bevoegd functionaris (BF) te hebben.
De bevoegd functionaris heeft onder andere de volgende taken:
- het doel van de artikel 9-verwerking omschrijven en vastleggen;
- het autoriseren van personen voor de betreffende verwerking;
- bepalen of gegevens voor andere doeleinden mogen worden gebruikt;
- zorgen dat voor alle gegevens de herkomst en wijze van verkrijgen wordt vastgelegd;
- bewaken dat gegevensrechtmatig worden verkregen en verwerkt.

8. Rechten van betrokkenen
De rechten van betrokkenen onder de AVG staan uitgebreid beschreven in het privacybeleid van de gemeente Nunspeet. Op hoofdlijnen zijn deze rechten op grond van de Wpg gelijkluidend. Specifiek voor de Wpg geldt nog het volgende:

Een verzoek om inzage, rectificatie of vernietiging wordt afgewezen voor zover dit noodzakelijk en evenredig is ter vermijding van belemmering van de gerechtelijke onderzoeken of procedures, ter vermijding van nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, ter bescherming van de openbare veiligheid, ter bescherming van de rechten en vrijheden van derden, ter bescherming van de nationale veiligheid en ingeval van een kennelijk ongegrond of buitensporig verzoek. Een gehele of gedeeltelijke afwijzing van een verzoek is schriftelijk en bevat de redenen voor de afwijzing.

9. Het bewaren van politiegegevens
Politiegegevens worden niet langer bewaard dan de minimale tijd die nodig is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt. Politiegegevens dienen na verwijdering nog maximaal vijf jaar worden bewaard. Indien van cultureel of historisch belang kan worden afgezien van vernietiging van de gegevens. Er wordt dan aan de bewaareisen als genoemd in de Archiefwet voldaan.
Alle politiegegevens worden gelabeld in artikel 8, 9 en 13 informatie. Voor elk label is de bewaartermijn conform de wettelijke bepaling geconfigureerd, zodat geborgd wordt dat deze politiegegevens niet langer worden bewaard dan de minimale tijd die nodig is, zoals vereist door de toepasselijke wet- en regelgeving, of voor de doeleinden waarvoor deze zijn verwerkt.

10. Het ter beschikking stellen en verstrekken van politiegegevens
De Wpg maakt een onderscheid tussen het ter beschikking stellen van politiegegevens en het verstrekken ervan. Het ter beschikking stellen van politiegegevens houdt in dat deze in principe worden gedeeld met eenieder die de gegevens nodig heeft voor de uitoefening van zijn taak. Bij dit 'need to know'-principe dient altijd een noodzakelijkheids-, proportionaliteits- en subsidiariteitsafweging te worden gemaakt. Het ter beschikking stellen voltrekt zich dus binnen het Wpg-domein.

Bij het verstrekken van politiegegevens gaat het om het delen van gegevens buiten het Wpg-domein. In dat geval moet zijn geborgd dat politiegegevens alleen worden verstrekt aan personen of instanties buiten het politiedomein, voor zover dit noodzakelijk is voor de doeleinden zoals deze in de Wpg en het Bpg zijn genoemd. Geborgd moet ook zijn dat wanneer gegevens verstrekt worden, er wordt voldaan aan de documentatieplicht en dat de verstrekking alleen plaatsvindt in overeenstemming met het bevoegd gezag indien dit vereist is in de wet. Het gaat dan bijvoorbeeld om verstrekkingen aan de burgemeester, een toezichthouder, een advocaat of een functionaris in het kader van de Wet bibob.

11. Het melden van datalekken
De datalek procedure onder de AVG staat beschreven in het protocol inzake privacy incidenten van de gemeente Nunspeet 2022. Op hoofdlijnen zijn deze rechten op grond van de Wpg gelijkluidend. Specifiek voor de Wpg geldt nog het volgende:

Op deze mededelingsplicht zijn enkele uitzonderingen van toepassing, onder andere als de mededeling achterwege moet blijven ter vermijding van belemmering van de gerechtelijke onderzoeken of procedures en ter vermijding van nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen.

12. Bewustwording
Het zorgvuldig omgaan met persoonsgegevens is enerzijds een kwestie van het organiseren van een goede informatieveiligheid en het zorgvuldig inrichten van werkprocessen, anderzijds is het een zaak

van bewustwording bij de boa's. Het bewustzijn wordt voortdurend aangescherpt, zodat kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd.
Elke nieuwe medewerker moet daarom verplicht een Wpg training doorlopen. Daarvan wordt een notitie vastgelegd in het personeelsdossier. Daarnaast ontvangt elke boa met terugwerkende kracht dezelfde presentatie. Deze keert jaarlijks terug. Ook daarvan wordt een notitie in het personeelsdossier gemaakt zodat de bewustwording geborgd wordt.

13. Open communicatie

Betrokkenen moeten erop kunnen vertrouwen dat hun persoonsgegevens zorgvuldig worden verwerkt. De gemeente Nunspeet creëert dat vertrouwen door inzichtelijk te maken, door middel van verschillende communicatiekanalen, op welke wijze hij persoonsgegevens verwerkt en beheert. Dit staat in de privacyverklaring die op de website is te vinden: www.nunspeet.nl/privacy-statement.